International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3655

(09/2022)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Big Data

Big data driven networking – Management and control mechanisms

Recommendation ITU-T Y.3655

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	**Y.3600–Y.3799**
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3655

Big data driven networking – Management and control mechanisms

Summary

Recommendation ITU-T Y.3655 specifies management and control (MC) mechanisms for big data driven networking (bDDN). Recommendation ITU-T Y.3655 studies, for bDDN, mechanisms related to general MC aspects, as well as specific management, control and orchestrations.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3655	2022-09-29	13	11.1002/1000/15062

Keywords

Big data, big data driven networking, control, management, mechanism.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3655

Big data driven networking – Management and control mechanisms

1 Scope

This Recommendation specifies mechanisms for management and control (MC) of big data driven networking (bDDN), including:

- an introduction;
- management mechanisms;
- control mechanisms;
- orchestration mechanisms;
- other related considerations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

[ITU-T Y.3653] Recommendation ITU-T Y.3653 (2021), *Big data-driven networking – Functional architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big-data-driven networking (bDDN) [b-ITU-T Y.3650]: A type of future network framework that collects big data from networks and applications, and generates big data intelligence based on the big data; it then provides big data intelligence to facilitate smarter and autonomous network management, operation, control, optimization and security, etc.

3.1.2 policy [b-ITU-T G.7701]: The set of one or more rules that define the action that an MC component takes in response to a set of conditions presented at an interface. More than one policy may be applied (sequentially) to these conditions to determine the final action taken by the MC component.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

bDDN Big Data Driven Networking

DNP	Dynamic Network Probe
E2E	End to End
gRPC	Google Remote Procedure Call
iBE	interface between Big data plane and External
iBM	interface between Big data plane and Management plane
iBN	interface between Big data plane and Network plane
KPI	Key Performance Indicator
MC	Management and Control
ML	Machine Learning
NETCONF	Network Configuration Protocol
NFV	Network Function Virtualization
NMF	Non-negative Matrix Factorization
NMS	Network Management System
OAM	Operations, Administration and Maintenance
OWAMP	One-Way Active Measurement Protocol
SNMP	Simple Network Management Protocol
VNF	Virtualized Network Function
YANG	Yet Another Next Generation

5 Conventions

This Recommendation uses the following conventions.

In this Recommendation, the auxiliary verbs "should", and "may" sometimes appear, in which case they are to be interpreted, respectively, as "is recommended", and "can optionally". The appearance of such phrases or words in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction of management and control mechanisms of bDDN

6.1 Overview of closed loop of management and control mechanisms

See clause 3.1.1 for a definition of big data driven networking (bDDN).

bDDN can increase efficiency while decreasing operating costs. bDDN uses big data sensing, big data analytics, machine learning (ML) methods and network intelligence-related methods to provide capability for self-discovery, self-analysing, self-configuration, self-healing, etc. As a result, bDDN can deliver optimized and customized quality of service inexpensively to the end user. The aim of the bDDN is to eliminate the manual work required to keep networks running. This is also the core target of the MC mechanisms of bDDN.

Network MC is a complex task and involves a cloud centre, core and metro transport network, mobile fronthaul and backhaul network, user applications, etc. It needs to consider not only optimization and orchestration mechanisms, but also running applications on such a diverse and distributed infrastructure. Even by using highly engineered network operational tools, it possibly takes several days or even weeks for upgrades or service deployments to take effect.

Software-defined networking introduces centrally controlled network programmability and software centric flexibility in contrast to traditional distributed control mode. However, the centralized SDN platform is largely focused on static network operations and manual driven control. In contrast to SDN, bDDN uses the big data plane to realize automatic discovery of problems and automatic configuration and optimization of the network.

Figure 6-1 shows the closed loop for MC in bDDN, where network infrastructure, physical or virtual, is continuously monitored using a sensing engine, and real-time network states are exposed to the analytics stage, which in turn feeds into the management plane. The bDDN control platform not only takes centralized and programmable control, but also deploys data driven automation with policy-based orchestration and management.

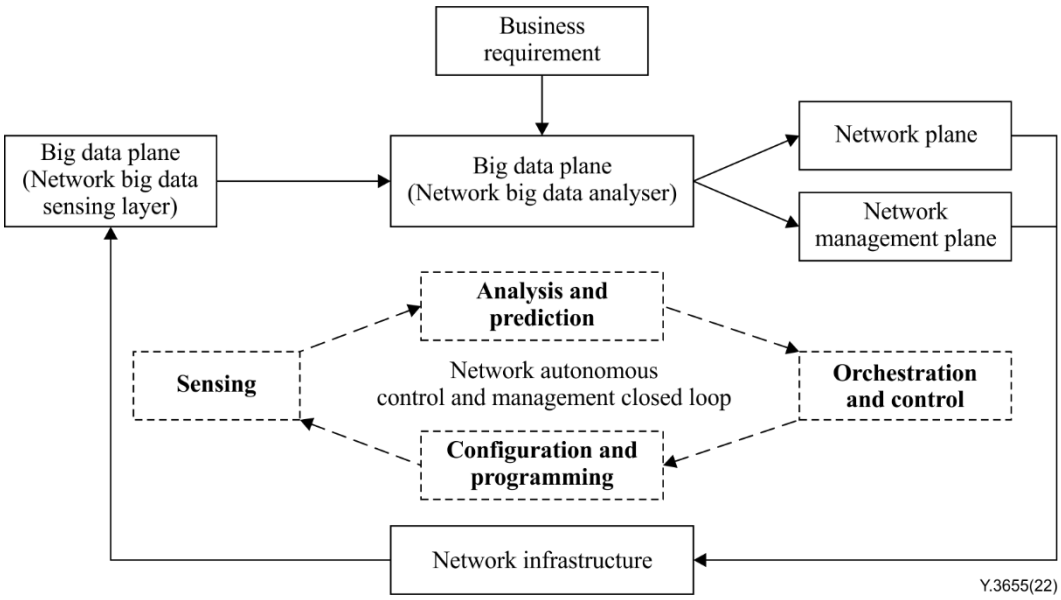


Figure 6-1 – Closed loop of control and management mechanisms

The big data plane is the brain of a network and is fundamental to intelligent networks that can support change in the level of service agility and adaptability. It enables lifecycle orchestration and automation for end-to-end (E2E), data driven network service, working in conjunction with the operation-supporting system and customer-facing support systems. In combination with analytics driven intelligence and policy control, the big data plane can help network service providers make the paradigm shift to the new mode of network operations that is based on sensing, analysis and prediction, orchestration and control, configuration and programming cycles, as shown in Figure 6-1. The sensing aspect monitors and collects network status data, such as network faults and network congestion. The analysis and prediction aspects decide using the big data analyser. The orchestration and control aspect schedules the resource according to the results of the analysis. The configuration and programming aspect self-configures or programs the infrastructure.

Note the importance of closed-loop operation for bDDN as it fundamentally changes the way networks are operated traditionally, empowering truly dynamic and autonomous operation.

6.2 Sensing aspect

Several bDDN mechanisms, which can be realized by a management protocol such as the simple network management protocol (SNMP), a management interface such as a client line interface and log tools such as Syslog, are provided to collect data from a network. These mechanisms have limitations that restrict automation and scalability. One limitation is the use of the pull model, where the initial request for data from network elements originates from the control or management entity. The pull model does not scale when there is more than one network management entity in the network.

With this model, the server (network element) sends data only when clients (control or management entity) request it. To initiate such requests, continual manual intervention is usually required. This continual manual intervention makes the pull model inefficient.

The active sensing model continuously streams data out of the network element and notifies control or management. bDDN supports the active sensing model and the pull model simultaneously, which provides near real-time access to monitoring data.

The active sensing data model has always been an important mechanism in bDDN.

6.3 Analysis and prediction aspect

The analysis and prediction aspect of bDDN makes corresponding decisions by analysing network status data and user requirements, especially service provisioning, traffic engineering, proactive maintenance, capacity planning and other scenarios.

The diversity of the future networking infrastructure, and the dynamic attribution of both the application and infrastructure layers require that bDDN be augmented with advanced active monitoring and ML analytics functionalities for E2E network management.

The goal of analysis and prediction is to incorporate intelligence via various ML and big data toolsets, and this intelligence includes learning hidden relationships, discovering traffic patterns, finding anomalous events and recommending actions.

Consider network capacity management as a specific example. The bDDN platform receives business and operational requirements as an input, and uses abstracted network topology and sensing data (e.g., traffic load, performance and deployed bandwidth) to adjust deployed network capacity. bDDN is expected to deliver substantial cost-saving and improved efficiencies, while minimizing engineering and testing efforts.

6.4 Orchestration and control aspect

Orchestration and control is a crucial process for network service provision. In conventional networks, service provision can take several hours or even days. Also, lifecycle management of network services often consists of a lot of expensive, inflexible, manual steps in hardware-based implementations. Consequently, there is a growing interest in network softwarization and network function virtualization (NFV), which aim to execute network service components as virtualized network functions (VNFs) on top of network infrastructures.

The big data plane carries out the mechanism for closed-loop automated workflows and autonomous actions based on predetermined policies and customer requirements. It manages and orchestrates network controllers, network resources and the programmable infrastructures through big data intelligence and open interfaces. For example, in provisioning an on-demand layer 1 transport service, the big data plane ingests and translates customer requirements from a self-service portal and provides automated discovery and selection of ports using service templates. It then calls a path computation element to find the best route and stitch.

6.5 Configuration and programming aspect

The network plane controller and infrastructure are essential to implement network programmability. The centralized network management and programmable flow control and device configuration in bDDN are crucial to the achievement of dynamic delivery of network connectivity services and automation of manual provisioning tasks. There are many disparate tools to increase network automation: cross-domain configurators for automated, multi-vendor device configuration; overlay controllers for traffic steering; and domain- or layer-specific controllers to automate the management of individual networks. bDDN converges these various models into a single, open and modular platform. It provides centralized and converged MC of multiple network layers that are traditionally managed separately. It also realizes E2E, multi-vendor network lifecycle automation.

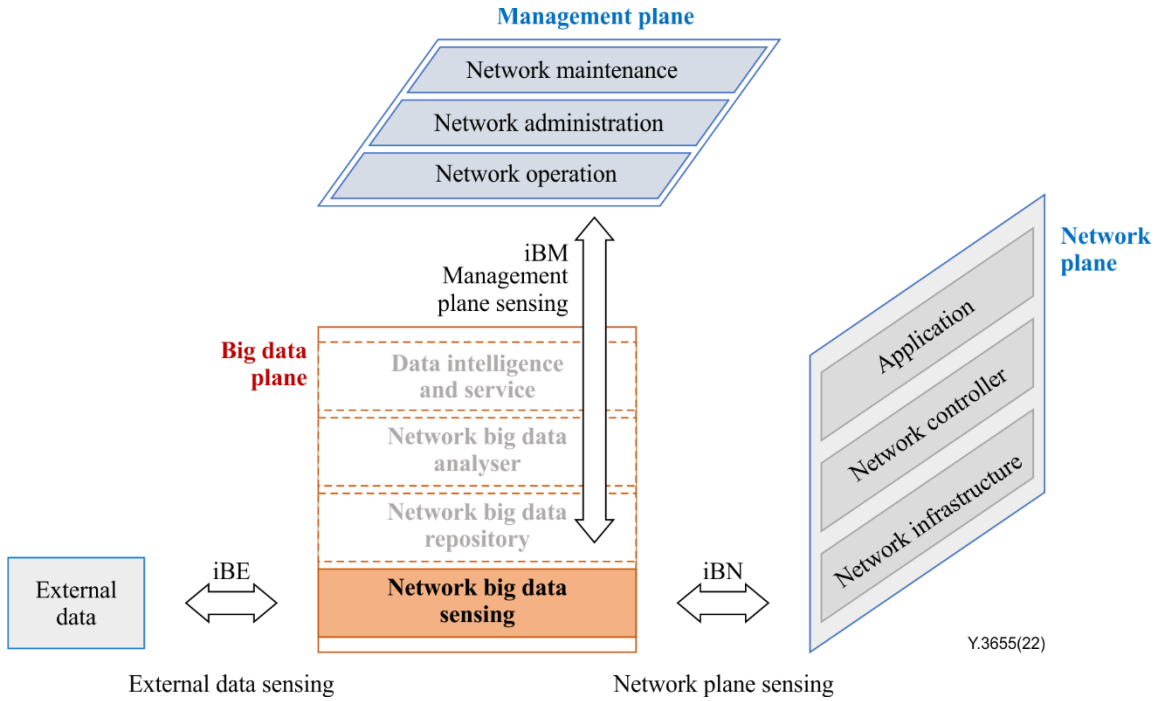
7 Active sensing mechanism of bDDN

Traditionally, network operators have relied upon protocols such as SNMP to monitor the network. SNMP can only provide limited information about the network. Since SNMP is pull mode based, it incurs a low data rate and high processing overhead. In bDDN, big data analytics and ML technologies are based on full state data from networks. Traditional SNMP technologies cannot meet full state data requirements.

Active sensing is that in push mode, which differs from the pull mode of traditional sensing. It is subscribed once and reported continuously and regularly. This active sensing method can improve real-time performance of sensing data and avoid the impact of pulling on the collector itself and network traffic. Active sensing can directly trigger automated network operation. Conventional operations, administration and maintenance (OAM) tools only help human operators to monitor and diagnose the networks and guide manual network operations.

7.1 Sensing interface

The active sensing module of a big data plane should collect data from the network and management planes in bDDN, as well as other external data out of the network, as shown in Figure 7-1.



iBE: interface between big data plane and external; iBM: interface between big data plane and management plane; iBN: interface between big data plane and network plane

Figure 7-1 – Collection data of the active sensing module

7.2 Management plane sensing

7.2.1 Interface of management plane sensing

The big data plane gets data from the management plane via the iBM interface.

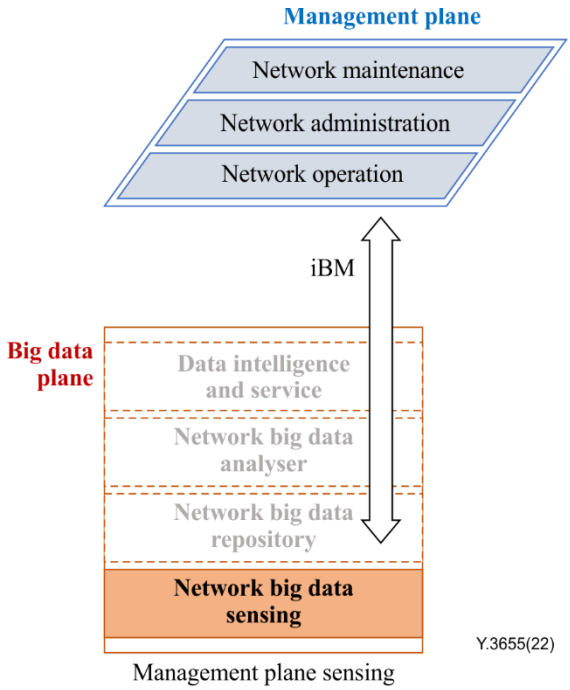


Figure 7-2 – Interface of management plane sensing

The protocol or method of iBM should have the following features.

– Convenient data subscription:

  an application chooses the data export means such as data type and export frequency.

– Data structuring:

  for automatic network operation, machines replace human operator for network data comprehension – the schema languages such as yet another next generation (YANG) [b-IETF RFC 6020] can efficiently describe structured data and normalize data encoding and transformation.

– High speed data transport:

  in order to retain the information efficiently, a server needs to send a large amount of data at high frequency – compact encoding formats are needed to compress the data and improve data transport efficiency.

7.2.2 Traditional sensing

The management plane of the network element interacts with the network management system (NMS), and provides information such as performance data, network logging data, network warning, faults data, network statistics and state data. Some traditional protocols are widely used for the management plane, such as SNMP and Syslog, these protocols can be also used in the bDDN.

7.2.3 Programmable sensing

In order to meet the requirement of automatic analysis and decision-making, a programmable sensing method is needed in bDDN.

1 Network configuration protocol

The network configuration protocol (NETCONF) [b-IETF RFC 6241] is one popular network management protocol. YANG push extends NETCONF and enables subscriber applications to request a continuous, customized stream of updates from YANG data storage. Providing such visibility into changes made upon YANG configuration and operational objects enables new capabilities based on the remote mirroring of configuration and operational state. Moreover, a

distributed data collection mechanism via a user datagram protocol-based publication channel provides enhanced efficiency for NETCONF-based telemetry.

2 Google remote procedure call network management interface

The Google remote procedure call (gRPC) is a modern open-source high-performance remote procedure call framework that can run in any environment. It can efficiently connect services in and across data centres with pluggable support for load balancing, tracing, health checking and authentication [b-gRPC]. A gRPC network management interface is a network management protocol based on the gRPC framework. With a single gRPC service definition, both configuration and telemetry can be covered. It supports a number of capabilities that make it well suited for active sensing, including the following.

– Full-duplex streaming transport model combined with a binary encoding mechanism provided for further improved telemetry efficiency.

– The gRPC provides higher-level feature consistency across platforms that common hypertext transfer protocol/2 libraries typically do not. This characteristic is especially valuable because telemetry data collectors normally reside on a large variety of platforms.

7.3 Network plane sensing

7.3.1 Interface of network plane sensing

The big data plane gets data from the management plane via the iBN interface.

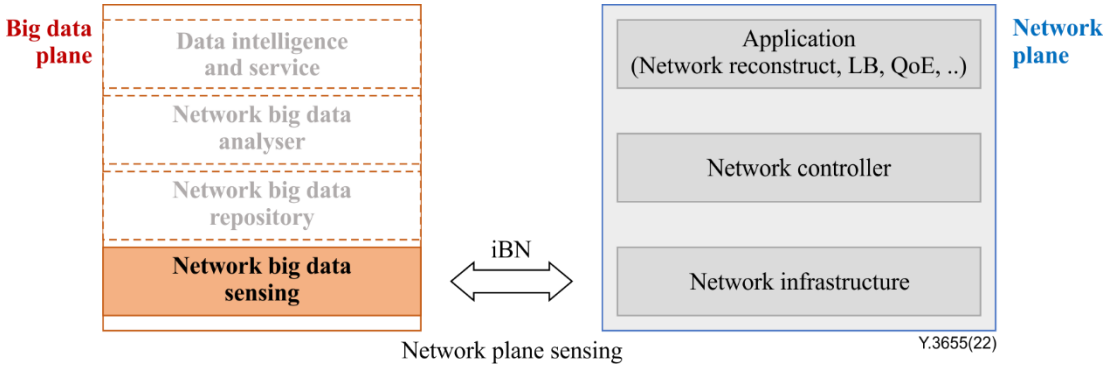


Figure 7-3 – Interface of network plane sensing

An effective network plane sensing system relies on the data that the network device can expose. The quality, quantity, and timeliness of the data must meet some stringent requirements. This raises some challenges to network plane devices where the first hand data originate.

The main function of a network plane device is user traffic processing and forwarding. Although it is important to support network visibility, the sensing function is just an auxiliary function and it should not impede normal traffic processing and forwarding (i.e., the performance should not be lowered and the network behaviour should not be altered due to telemetry functions). Network operation applications require E2E visibility from various sources, which results in a huge volume of data. However, the collected data quantity should not stress the network bandwidth, regardless of the data delivery approach (i.e., through in-band or out-of-band channels).

Network plane devices must provide data in a timely manner with the minimum possible delay. Delays in processing, transport, storage and analysis can impact the effectiveness of the control loop and even render the data useless. Network plane devices need to provide enough flexibility and programmability to support precise data provision for applications. Network plane telemetry should support incremental deployment even though some devices are unaware of the system. This challenge is highly relevant to legacy networks.

In the network plane, controller and application also need sensing. Controller and application sensing involves monitoring the condition, such as availability, of application and different network protocols, which cover layer 2 to layer 7. Keeping track of the running status of these protocols is beneficial for detecting, localizing and even predicting various network issues, as well as network optimization, in real time and in fine granularity.

7.3.2 Traditional sensing

Traditional methods include Internet protocol flow information export [b-IETF RFC 5103], sFlow [b-IETF RFC 3176] and traffic mirror. These methods usually have low data coverage. In contrast, active methods such as the one-way active measurement protocol [b-IETF RFC 4656], the two-way active measurement protocol [b-IETF RFC 5357] are intrusive and only provide indirect network measurement results. Hybrid methods, including *in-situ* OAM [b-IETF RFC 9197] and multipoint alternate marking [b-IETF RFC 8889], provide a well-balanced and more flexible approach. These methods can also be used in bDDN.

7.3.3 Dynamic network probe

A hardware-based dynamic network probe (DNP) provides a programmable means to customize the data that an application collects from the network plane. A direct benefit of DNP is the reduction in volume of exported data. A full DNP solution covers several components including source, subscription and generation of data. The data subscription needs to designate the custom data that can be composed and derived from raw data sources. Data generation takes advantage of the moderate in-network computing to produce the data desired. While DNP can introduce unforeseeable flexibility in data plane telemetry, it also faces some challenges. It requires a flexible data plane that can be dynamically reprogrammed at run time.

7.4 External data and event sensing

The big data plane gets data from the management plane via the iBE interface.

Events that occur outside the boundaries of the network system are another important source of telemetry information. As with other sources of telemetry information, data and events must meet strict requirements, especially in terms of timeliness, which is essential to properly incorporate external event information into management cycles.

The role of external event detector can be played by multiple elements, including hardware and software. Since the main function of external event detectors is actually to notify, their timeliness is assumed. However, once messages have been dispatched, they must be quickly collected and inserted into the control plane with variable priority, which is high for important sources or important events and low for secondary ones. The ontology used by external detectors must be easily adopted by current and future devices and applications. Therefore, it must be easily mapped to current information models, e.g., in terms of YANG.

Organizing both internal and external telemetry information together is key to general exploitation of the management possibilities of current and future network systems, as reflected in the incorporation of cognitive capabilities to new hardware and software (virtual) elements.

8 Data analysis mechanism of bDDN

With the improvement in network sensing ability, there is abundant knowledge hidden in massive network data. This knowledge reveals the laws of network operation and user behaviour. It is also very important for network MC. The big data plane of bDDN uses data analysis and mining methods to produce the knowledge and provide it to the network management and network planes.

8.1 Data analysis function

The bDDN discovers the knowledge, in other words trends in network operation and user behaviour, by analysing massive service data and performance data generated in the communication process.

8.2 Data analysis mechanism

Network data analysis and knowledge discovery can be divided into four modules for: data extraction; data pre-processing; knowledge discovery; and result analysis. Each module can be further subdivided as shown in Figure 8-1.

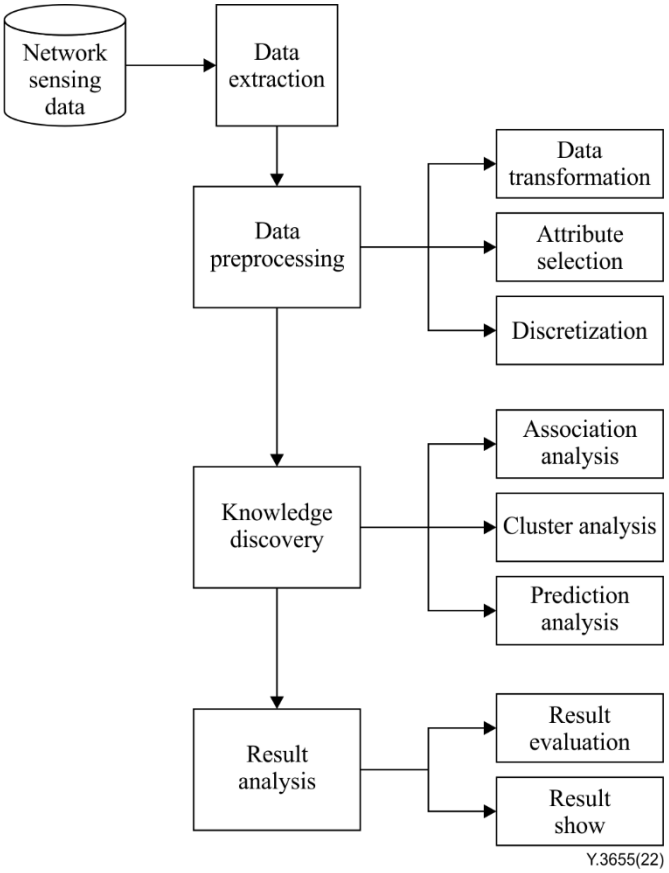


Figure 8-1 – Mechanism of data analysis and knowledge discovery

1 Data extraction

The data extraction procedure involves inputting data from different data sources into the big data repository of a big data plane. Different extraction methods may be used to maximize data processing efficiency.

2 Data pre-processing

A data pre-processing procedure can obtain a simple representation of data sets and greatly reduce the amount of data. Moreover, it can still maintain the integrity of the original data, and can produce almost the same mining analysis results. The main methods of data pre-processing include: data transformation; attribute selection; and discretization of continuous attributes.

A data transformation procedure changes source data into data that meets data quality requirements of according to predetermined rules.

Attribute selection chooses helpful attributes from the total, so as to avoid the situation in which all of them have to be introduced into the model for learning. Attribute selection is completely independent of any ML algorithm. It selects attributes according to statistical and correlation indicators.

A data discretization procedure is carried out for continuous data. After discretization, the data value domain distribution changes from one of continuous to discrete attributes.

3 Knowledge discovery

Knowledge discovery is the most important procedure. Various data-mining technologies can be used for different tasks. The main data-mining method are listed in (1) to (3) as follows.

(1) Correlation analysis

This analysis is mainly used to identify relationships among values of two or more variables, i.e., correlation. Correlation can be divided into the following types: simple; temporal sequential; and causal. Alternative methods are: the association rule-mining algorithm and its improved version; the decision tree generation algorithm for learning; and the use rule generation algorithm to formulate rules.

(2) Cluster analysis

This analysis classifies data into several categories according to similarity. Data in the same category are similar to each other, while data in different categories vary. Cluster analysis can identify a distribution pattern in data and a possible relationship between data attributes. The most famous and commonly used methods of cluster analysis are the C-means and its extended fuzzy C-means algorithms.

(3) Complex knowledge mining

The connectivity of large-scale networks is very complex. The network is composed of several groups. The connectivity between nodes in each group is relatively dense, but the connectivity between groups is relatively sparse. The discovery of connectivity plays an important role in guaranteeing communication, and provides data support for fault location and other tasks.

4 Result analysis

Mined knowledge should be evaluated and expressed in understandable ways, e.g., in the form of a decision table, decision tree, association rule and numerical prediction tree. The key technology is visualization. Visualization includes result visualization and process visualization.

9 Control mechanism of bDDN

9.1 Control closed loop in bDDN

bDDN can augment operational automation enabled by multi-domain orchestration with enhanced analytics and policy-controlled autonomous decision making. bDDN can provide advanced, embedded analytics capabilities in their networks that can aid self-learning from fast changing environments; provide accurate predictions of potential network problems and anticipate trends; and ensure continuous improvement and adaptation of rules that govern autonomous operations. Figure 9-1 provides an illustrative analytics and intelligence architecture for closed-loop automated operations in bDDN.

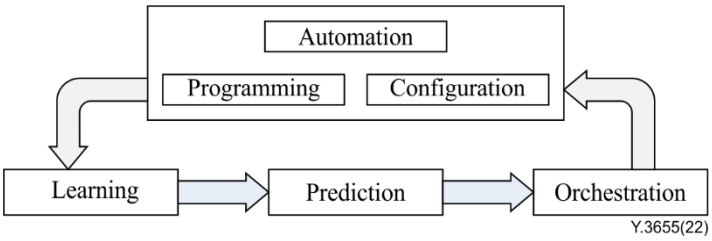


Figure 9-1 – Control closed loop in bDDN

In a big data plane, there is a robust storage repository that will record, process and aggregate real-time and historical large scale, raw data streams (such as log files and telemetry data) across the programmable infrastructure. This raw data should be processed, normalized and fed into the upper layers where advanced data models and analytics algorithms are used to generate operable insights. Artificial intelligence and ML are general-purpose technologies; providers will need to apply a variety of ML technologies based on the specific operational use cases and benefits they would like to achieve. Examples follow.

– Supervised learning: supervised ML algorithms can be trained to identify patterns (e.g., degrading network performance), predict an outcome (e.g., port failure), trigger remediation actions (e.g., auto-adjust network bandwidth, add new capacity). This type of ML is more commonly used and is suited for scenarios where historical data and outcomes are known.
– Reinforcement learning: involves continuous calibration of the ML algorithms based on feedback from its previous actions.
– Unsupervised learning: these algorithms use clusters to organize data to understand potential structures and enable the discovery of previously unknown or unnoticed patterns, i.e., identify new user or service traffic behaviour or profiles to improve forecasting in network planning.

Policy control and ML in a big data plane will collectively enable providers to design autonomous and adaptable troubleshooting, repair, configuration and mitigation processes. A policy module incorporates the intent-based rules and conditions set by the provider and intelligently governs the behaviour of the network. In a closed-loop automated process, the big data plane evaluates the events, insights and recommended actions from ML systems and triggers the appropriate response through the software control layer. As the network continues to learn from its actions over time, these policies can be adjusted and updated to adapt the network to changes as dynamically as the provider comfort level dictates.

9.2 Control procedure based on machine learning in bDDN

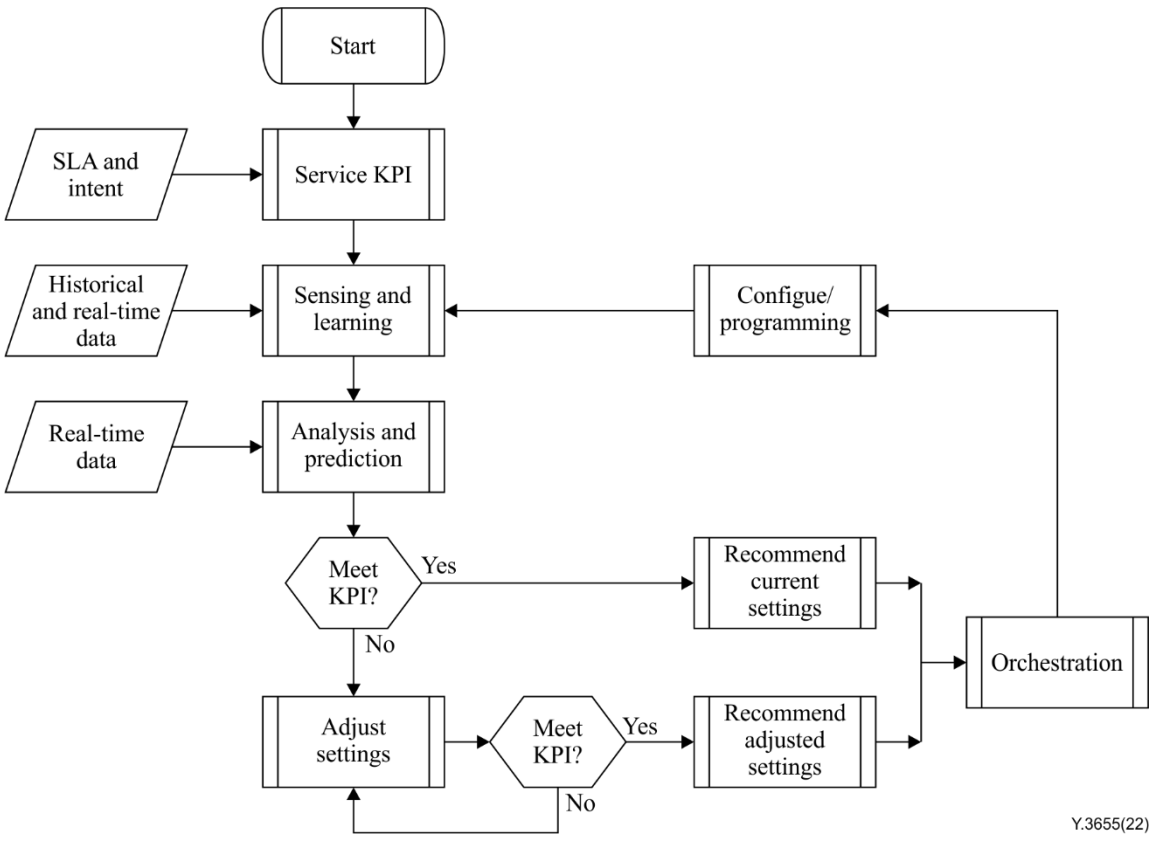


Figure 9-2 – Control procedure based on machine learning in bDDN

In the control procedure, the service quality of the network is represented by service key performance indicators (KPIs). First, user requirements or service level agreement are transformed into service KPIs. Then the sensing module collects network data. It will also compute and predict the network state and service level according to these data. The big data plane will judge whether the current policy meets the prevailing KPIs according to analysis results. If it is satisfied, the current control parameters and policies are recommended, and the policies sent to the orchestration module, which applies the policies and schedules the related resources. If it is not, the analyser shall give suggestions for adjusting the policy control parameters. According to the suggestions for its adjustment, the policy is recalculated to see whether the current KPIs are met. If they are not, iterative adjustments are needed. If they are, the policy is applied or set.

The learning procedure consists of the following steps:

– capture, storage, analysis and correlation of a real-time and historical network and service data, including structured data and unstructured data;
– construction of algorithms and application of ML technologies to identify patterns and extract new insight;
– support for changing situations with unpredictable data sets and achievement of self-learning.

The prediction procedure consists of the following steps:

– detection of anomalies to anticipate and avoid service disruptions and threats;
– support for performance assurance and customer care;
– analysis of traffic trends and capacity requirements to support proactive network planning;
– provision of recommendations for optimal human decision making.

The adjustment procedure consists of the following steps:

– dynamic updating of: models, rules and policies based on positive and negative; reinforcements for continuous improvement;
– guarantee of consistent change management through interworking with the software control layer.

The orchestration procedure consists of the following steps:

– scheduling of related resources according to the policy and settings, and configuration of the related module and device.

9.3 Artificial intelligence from the big data plane

9.3.1 Big data intelligence to the network and service control

Network and service control contains multi-dimension convergent MC functions to manage and control traditional and emerging networks. Intelligence from a big data plane includes intelligent network management, network optimization, automatic parameter configuration and intelligent transmission route optimization. At the same time, the ML training capability can be considered to meet requirements for fast-changing and highly real-time dependent service policy control. Big data intelligence can greatly reduce the cost of network operation and maintenance, and significantly improve the efficiency and convenience of network operation.

9.3.2 Big data intelligence to the network operation and orchestration

The operation and orchestration functions mainly include service and resource design, scheduling and management such as globe service orchestration and global resource orchestration.

With the big data plane of bDDN, orchestration systems can improve automation and intelligence capability for service orchestration, so as to make network change on-demand based on dynamic and

intelligent strategies, and make intelligent predictions for service volume change, as well as planning and managing related resources dynamically.

10 Management mechanisms of bDDN

The management plane of bDDN is responsible for network anomaly prediction, fault analysis and diagnosis, as well as intelligent network planning through big data analysis and ML technology.

10.1 Network anomaly prediction based on data

The performance indicator of a network directly reflects its status, reliability, availability and quality. Any fault in the equipment, link and software system in the network is reflected in performance data. The goal of anomaly prediction is to estimate the possibility of the occurrence of a fault before it occurs, and to formulate an emergency plan when it does. In bDDN, the management plane is able to effectively manage unknown and predictable serious events based on the big data plane, i.e., the management plane has the ability of active prediction, to provide the basis for network administrators to make decisions and take defence measures, so as to prevent accidents in advance.

1 The function of network anomaly prediction

Because many network performance indicators have the characteristics of time accumulation and space superposition, bDDN can find signs of network anomalies from trends in network performance change, and predict the occurrence of network anomalies. Network anomalies include congestion, a large number of call failures, insufficient resources or capacity and network attack events. In addition, the management plane of bDDN can infer the further influence of an abnormal situation on the network according to the status of the current network, such as a sudden decline in network performance or the failure of network equipment. For example, the failure of a device spreads a network performance abnormality from local to global, and the failure or abnormality of a system may affect the performance of other systems. The NMS shall be able to predict the scope, speed and influence degree of abnormal or fault diffusion, and put forward appropriate preventive measures and suggestions.

2 The mechanism of network anomaly prediction

Prediction is the use of historical data to identify trends of change, in other words, prediction constructs a model to foresee the characteristics of future data. Anomaly prediction is to estimate the possibility of an event before it occurs. It requires that. in the process of analysing and learning from past performance data, rules of change and trends in values of time series observations be identified, as well as their relationship with faults or abnormal events. The prediction value is then determined, as well as the probability of an abnormal event by extrapolating these rules or trends.

The performance-based network anomaly prediction mechanism assumes that one or several network performance data are in a time series, $x = \{x_i | x_i \in R, i = 1, 2 \ldots L\}$; network early warning can be achieved by using the time series prediction model. The future m values can be predicted through the past values of the first n times of the sequence. Time series prediction methods include classical statistical methods, artificial neural networks and other ML methods.

For anomaly prediction, bDDN automatically establishes a normal network performance model from the long-term performance history data of normal network operation by data mining and ML technology. By means of anomaly detection, such as single classification technology or semi-supervision technology, a network performance anomaly can be found in time, and its indicators can be presented to network management personnel by data visualization technology; the conceptual description of a network performance anomaly can also be provided (which indicators are abnormal, how they are abnormal, etc.). bDDN can provide supervision information for network performance data, and improve the accuracy of anomaly detection by the semi-supervised learning method using expert confirmation and denial. Handling suggestions can be saved to the expert database, which can automatically retrieve them for similar exceptions in the future. Network management personnel can

choose this suggestion or modify it, and use an ML method to continuously improve the expert database.

10.2 Fault diagnosis based on alarm and performance event

Fault diagnosis is always an important task of the management plane. Fault analysis and diagnosis based on artificial intelligence can deal with fault events more quickly than experts, and does not miss any clues.

1 Fault diagnosis function

In the case of network equipment failure, relevant equipment discovers it and issues a warning. However, there are also alarms of some faults that may not be given in time that affect network performance and result in performance events.

(1) Fault analysis and diagnosis based on performance data

It is difficult for a single network performance indicator to directly reflect the failure of a specific device or system.

Therefore, use is necessary of ML, pattern recognition and other technologies to analyse a large number of network performance data (including traffic volume, connection rate, average talk time, circuit utilization rate, average delay, average queue length and buffer occupancy rate). It is necessary to extract hidden information about the network state so as to discover a fault in advance, determine its type and location in the network and even make suggestions for troubleshooting.

(2) Fault analysis and diagnosis based on alarm events

Network alarm events are usually caused by network anomalies or faults that are usually detected by one or more related devices. Through event correlation analysis, several events may be merged or transformed into a composite event with more information, which can more directly and accurately reflect the root cause of fault events. On this basis, fault analysis and diagnosis should be combined with a device status and network structure to further locate specific fault device and fault causes. According to the results of the analysis, possible faulty device components and the corresponding possibilities are listed.

(3) Fault analysis and diagnosis based on performance and alarm

Sometimes, using performance statistics or an alarm event alone cannot locate the fault accurately. bDDN can combine these two aspects of information to carry out joint fault analysis and diagnosis to improve the accuracy of fault location.

(4) Heuristic troubleshooting based on test

Fault analysis and diagnosis by intelligent methods often provide the network operator with only a collection of possible fault sources, causes and confidence, which needs to be further investigated and diagnosed through tests with the participation of network management personnel. Heuristic fault analysis and diagnosis guide network management personnel to test the network according to the process, and provide more detailed and targeted data for the fault diagnosis system, so as to determine an achieve accurate fault location.

2 Fault diagnosis mechanism

The fault analysis module based on performance data uses anomaly detection technology to automatically confirm suspected network faults from performance data. Anomaly detection is the identification of a small number of abnormal patterns from the data, which rarely or even never appear in training samples. These abnormal patterns or anomalies are also known as outliers, novelties or novel points. The main detection technologies available are probability statistics, clustering, artificial neural network, single classification and decision tree.

Based on the event sequence and set generated by the event correlation and filtering module, the fault analysis module further integrates network configuration information, as well as the events and network states from different systems, by using decision tree, Bayesian network, association rule mining, sequence pattern recognition and fault propagation model combined analysis, to locate the cause of the failure, and obtain the set of possible failure sources, causes and corresponding confidence levels.

It is possible to improve the accuracy of fault location diagnosis by combining performance data and event information, but the time and space complexity is higher and the steps are more complicated.

Heuristic fault analysis and diagnosis identifies the test process from the diagnosis case base, guides network management personnel to test the network according to a certain process in the way of a wizard in which the test data is automatically collected by the system or supplemented by manual feedback to the fault analysis and diagnosis data set, and uses the decision tree algorithm to test various test results and network status and carry out classification analysis to finally locate the cause of failure. The final result is fed back to the fault analysis module as supervised data to train the classifier. The relationship of the fault analysis functions module is shown in Figure 10-1. Data sources include performance data, alarm or event data, network configuration data, network structure data and network service data. Fault analysis is based on all data after correlation and filtering. Heuristic analysis is based on the results of fault analysis, but heuristic analysis feed backs its own results to the fault analysis aspect as supervised data to the analysis module for training classifiers.

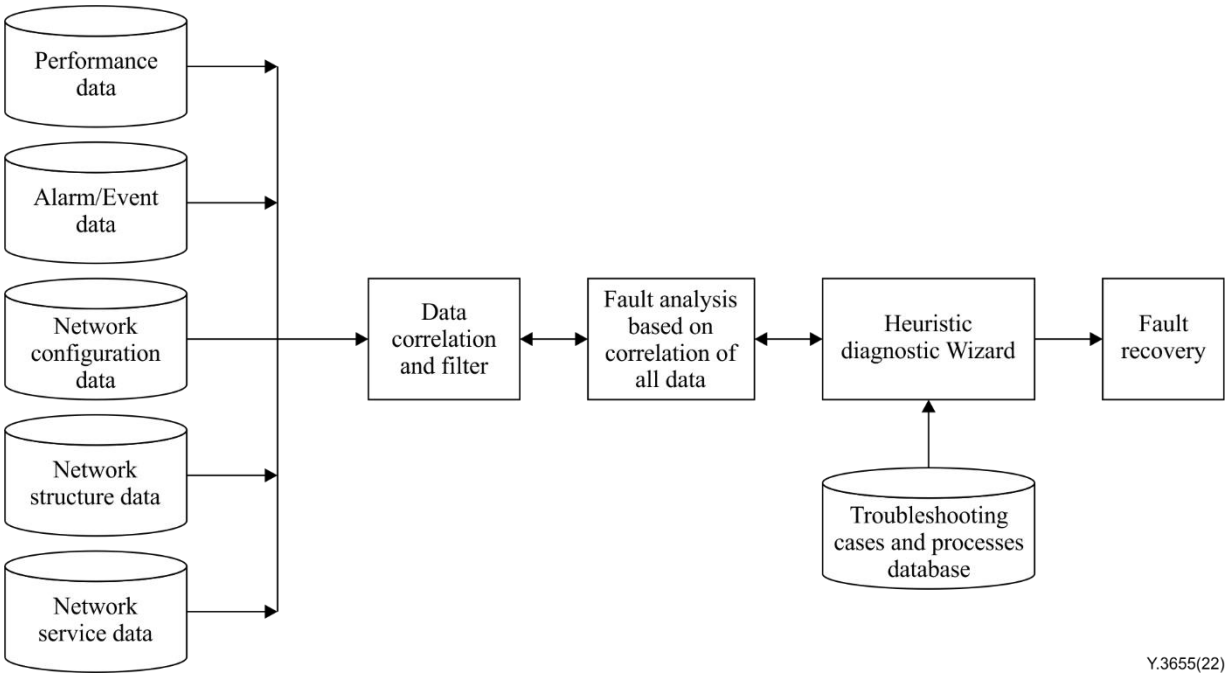


Figure 10-1 – Mechanism of fault diagnosis

10.3 Network intelligent planning based on community discovery

Due to the uneven distribution of network users, the uncertainty of network use, the imbalance of network resources and service configuration, the network is full of a large number of instances of unreasonable traffic and repeated invalid traffic. In traditional and emerging networks, applications and user behaviour often show a strong community structure, i.e., communication among users in the same community is frequent, while that between users in different ones is relatively sparse. Community discovery is the process of obtaining the community ownership relationship of users based on their connected records or related data analysis. According to the community structure, users belonging to the same community are planned in the same network, which will effectively reduce unreasonable traffic within it, so as to improve its efficiency and service quality.

1 Network intelligent planning functions

According to the actual communication data of its users, a community discovery algorithm is used to mine the community structure of the network. Based on community division results, the network is intelligently organized, and users with a close communication relationship are grouped in one network, so as to reduce communication delay and resource consumption. In addition, considering the network traffic type (text, voice, image and video) of network users, the priority of communication data, communication security level and other factors, allows a multi-attribute network to be intelligently planned. According to its dynamic characteristics, bDDN can sense changes in network structure in real time, and can automatically track and obtain its dynamic community structure. bDDN has the function of real-time and dynamic network planning.

2 Network intelligent planning mechanism

The user communication data in the network is extracted, and the communication frequency (or traffic) matrix that can reflect the network communication relationship is constructed. On this basis, the community structure is mined.

Sometimes, effective planning cannot be achieved depending solely on the communication relationships of a network, because it is usually sparse and the available information is limited: its nodes often have their own attributes, such as network traffic type, fixed service object and network attributes. The combination of attributes and connection information of a network can provide a more accurate and robust planning scheme. Because the data on link relationships and node properties are heterogeneous, the key to solving the problem of community discovery involves integration of the two kinds of data. The basic technical framework is shown in Figure 10-2.

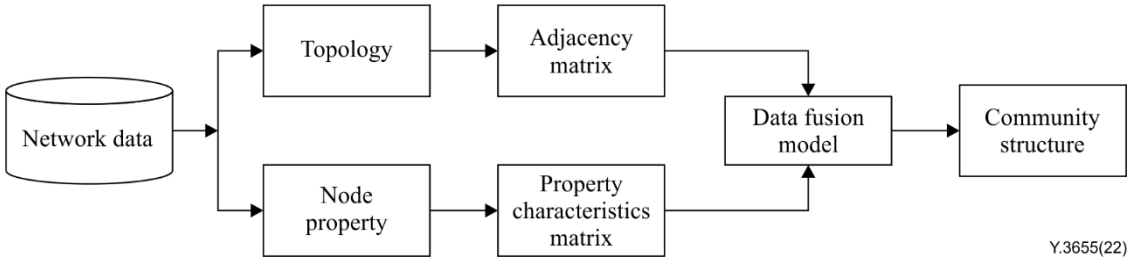


Figure 10-2 – Mechanism of community discovery

The data fusion model can be implemented in many ways, such as non-negative matrix factorization (NMF), graph embedding and graph neural networking. Because of its flexible model and strong physical interpretation, NMF can usually be used to achieve this heterogeneous data fusion. The basic idea is to transform attribute data into relational data according to the similarity measurement of the former, and then integrate with linked relational data to discover a community. The method of graph embedding maintains the structure information of a graph and represents it as a low dimension vector, aiming at mining useful information from its data, making it easier to extract meaningful information such as community when constructing a classifier or completing other tasks.

11 Orchestration mechanisms of bDDN

In bDDN, all operations and control of the network are implemented by the network plane. The network plane also needs to complete the coordination and orchestration of these operations. This is accomplished by the orchestration module of the network plane.

According to the scope of the resources involved, resource orchestration can be divided into two modes:

- one domain;
- multi-domain.

11.1 One domain resource orchestration

Figure 11-1 illustrates a one domain multi-network orchestration functional block. It consists of three parts:

- one domain unified policy centre;
- one domain unified resource centre;
- resource orchestrator.

In bDDN, some operations of the network management plane need to be realized by the controller of the network plane. From this point, the applications of network management have the same effect as those of business.

All requests about operation or control from the management plane to the network plane become the policy of the network to be implemented in its plane. In bDDN, a unified policy management mechanism is adopted in the network plane. bDDN describes the policy in a unified way to realize the MC of the whole network and the automation of network operation, maintenance and management. In bDDN, the unified policy centre of the orchestration module in the network plane is used for policy processing. The network plane of bDDN adopts the method of centralized and unified management of resources, which is not only compatible with the bDDN centralized control framework, but also concentrates the control of resources, enabling them to be shared among devices and improve efficiency. bDDN has the programmable characteristics by using NFV and other programmable technologies.

In bDDN, a resource orchestrator is responsible for resource allocation and policy computation. It constructs the model according to the relevant information from a unified resource centre and unified policy centre, and deploys and schedules VNFs.

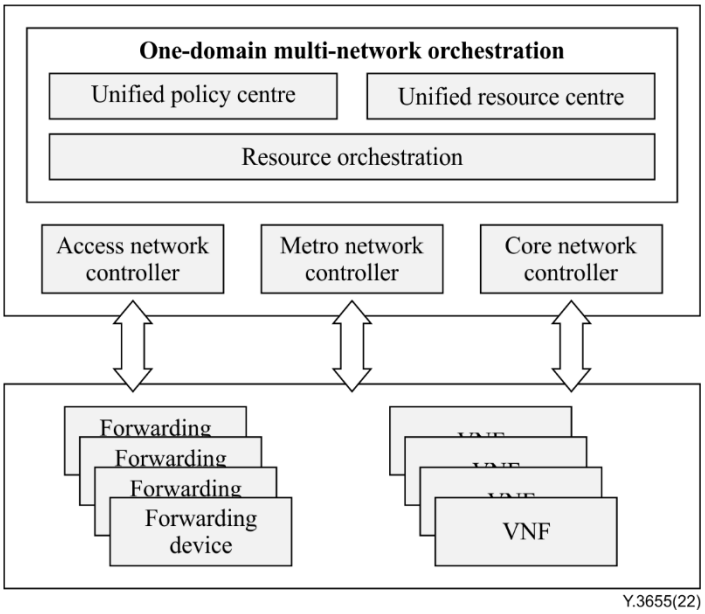


Figure 11-1 – One domain orchestration functional block

11.2 Multi-domain resource orchestration

An E2E service or application is always deployed across multiple domains. The process of establishing a multi-domain network service leverages the benefits of resource virtualization and cross-domain resource orchestration.

Figure 11-2 depicts a fully functional E2E service across three domains, illustrating the respective physical or virtual infrastructure. Cross-multi-domain resource orchestration involves two or more network controllers that belong to different domains. The main process is as follows.

1) Mapping of the service requirements on to capability requirements by the service management module in the network plane [ITU-T Y.3653].

2) Translation of the capability requirements by multi-domain unified resource centre into:

   a) resource requirements in terms of computing, storage and networking resources;

   b) topology and connectivity type, policy, isolation and security requirements.

3) Identification of the domains with the required resources by multi-domain unified resource centre.

4) Allocation of resources in each domain and then assignment of these resources to the service by a one domain unified resource centre.

5) Coordination operations across different domains to maintain E2E service integrity by the multi-domain unified resource centre.

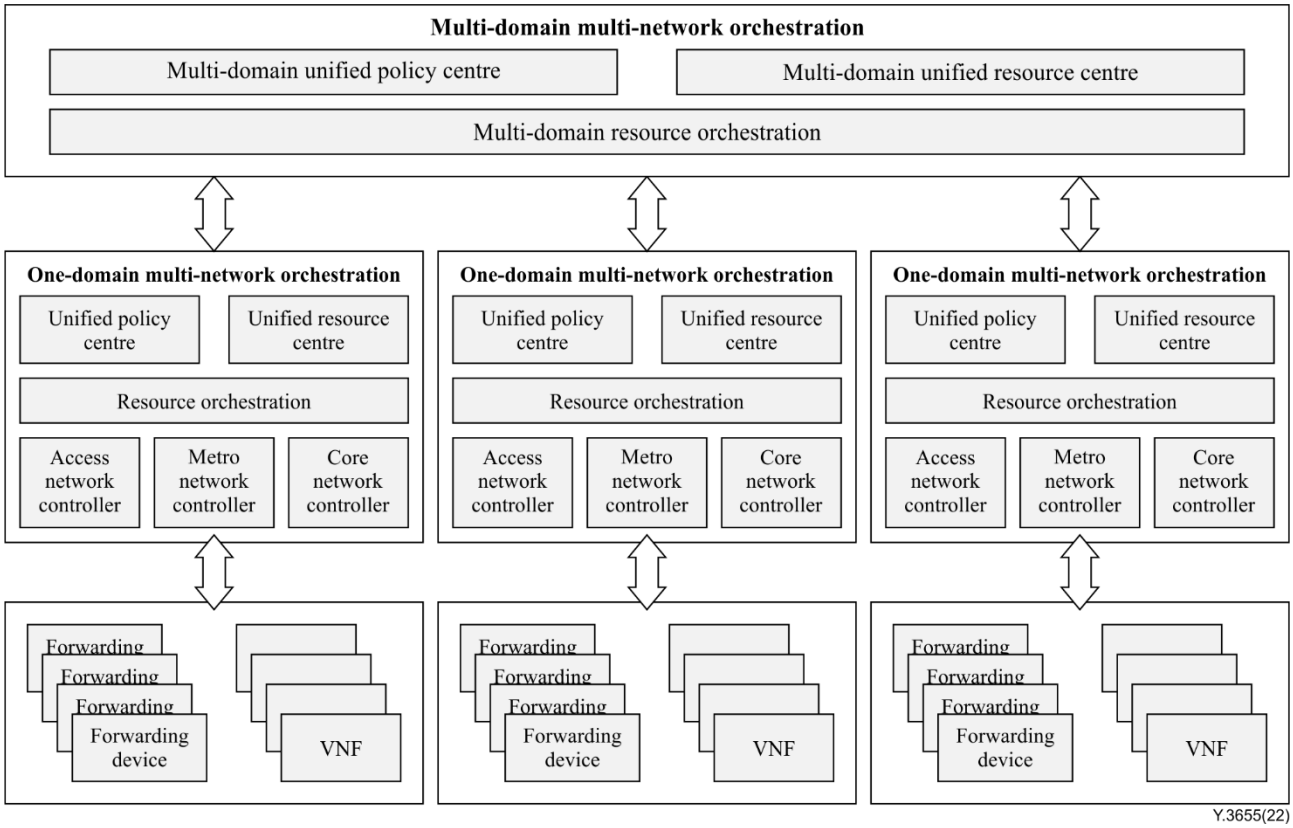


Figure 11-2 – Multi-domain orchestration functional module

The multi-domain orchestration module is responsible for resource orchestration and management across different domains. It consists of three main building blocks: the multi-domain orchestrator; the multi-domain unified policy centre; and multi-domain unified resource centre.

The multi-domain resource orchestrator decomposes a resource request and directs the components to different administrative domains and decides on their combination, also including also cross-domain connectivity. It also carries out potential service specific re-adjustments and modification across different domains, as well as decommissioning domains upon request if performance degrades or service policy is updated. The multi-domain orchestrator analyses related service requirements and contacts the appropriate sub-level domains negotiating resources. A multi-domain resource orchestrator allocates cross-domain computation, storage and network resources with the help of a unified policy centre and a unified resource centre.

The multi-domain unified policy centre interprets and translates the service requests for the heterogeneous resource description. The unified resource centre also manages cross-domain computation, storage and network connectivity resources across different administrative domains. Logical resources from different domains are collected by the unified resource centre.

12 Security considerations

When using bDDN, security best practices should be adopted, such as authentication, authorization and access control as described in [ITU-T Y.2704].

In the meantime, operations related to network resources should have multiple reliability guarantees to avoid incorrect operation of network resources and degradation in network performance.

Bibliography

[b-ITU-T G.7701] Recommendation ITU-T G.7701 (2022), *Common control aspects*.

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[b-ITU-T X.731] Recommendation ITU-T X.731 (1992), *Information technology – Open Systems Interconnection – Systems management: State management function*.

[b-ITU-T Y.3650] Recommendation ITU-T Y.3650 (2018), *Framework of big-data-driven networking*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A method for monitoring traffic in switched and routed networks*.

[b-IETF RFC 4656] IETF RFC 4656 (2006), *A one-way active measurement protocol (OWAMP)*.

[b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional flow export using IP flow information export (IPFIX)*.

[b-IETF RFC 5357] IETF RFC 5357 (2008), *A two-way active measurement protocol (TWAMP)*.

[b-IETF RFC 6241] IETF RFC 6241 (2011), *Network configuration protocol (NETCONF)*.

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modelling language for the network configuration protocol (NETCONF)*.

[b-IETF RFC 8889] IETF RFC 8889 (2020), *Multipoint alternate-marking method for passive and hybrid performance monitoring*.

[b-IETF RFC 9197] IETF RFC 9197 (2022), *Data fields for* in situ *operations, administration, and maintenance (IOAM)*.

[b-gRPC] gRPC (2022). *Introduction to gRPC.* Internet: gRPC. Available [viewed 2022-11-17] at: https://grpc.io/docs/what-is-grpc/introduction/.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022